REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-6 were pending in this application. By way of this reply, claims 7-16 have been added. Claim 1 is independent. The remaining claims depend, directly or indirectly, from claim 1.

Claim Amendments

Independent claim 1 has been amended by way of this reply. No new matter has been added by way of this amendment, as support for this amendment may be found, for example, on page 11, line 30 – page 12, line 21 of the present application.

Claims 3-6 have been amended to remove multiple dependencies. Additionally, claim 4 has been amended to clarify that a display device is one selected from the group consisting of a printer, a screen, and a filing device. Additionally, claim 5 has been amended to clarify that a protected device sends a display device result data of a certificate. Claims 1-6 have been amended to remove reference numerals. No new matter has been added by way of these amendments.

New Claims

New claims 7-16 have been added to correspond to the removal of multiple dependencies in claims 3-6. No new matter has been added by way of these amendments.

Specification Amendments

The amendments to the specification have been made to clarify the invention by correcting translation errors. No new matter has been added by way of these amendments.

Objections

The abstract of the disclosure was objected to for containing legal phraseology such as "means" and "said." By way of this reply, the abstract of the disclosure has been amended to remove instances of "means" and "said." Additionally, the abstract of the disclosure was objected to because it was unclear what was meant by the last 3 lines in the abstract, "Application for protecting exchanges on communication networks. (Figure 1)." By way of this reply, the abstract has been amended to remove these lines. Accordingly, withdrawal of any objections to the abstract is respectfully requested.

Claims 4-6 are objected to as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claim. By way of this reply, claims 4-6 have been amended remove multiple dependencies. Accordingly, claims 4-6 no longer depend from multiple claims, and withdrawal of the objection to claims 4-6 is respectfully requested.

Rejection(s) under 35 U.S.C. § 112

Claim 5 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. Claim 5 has been amended in this reply to remove the phrase "such as the date of validity of the certificate." Accordingly, withdrawal of the rejection of claim 5 is respectfully requested.

Rejection(s) under 35 U.S.C. § 103

Claims 1-3 are rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,170,058 issued to Kausik (hereinafter "Kausik") in view of U.S. Patent No. 4,529,870 issued to Chaum (hereinafter "Chaum"). Independent claim 1 has been amended in this reply to clarify the present invention recited. To the extent that this rejection may still apply to the amended claims, the rejection is respectfully traversed.

The present invention is directed to a method for checking the signature of a message. As discussed with reference to Figure 1 of the Specification, in one embodiment of the invention, a system for authenticating a message during cryptographic processing of the message comprises a computer (10), a protected device (21), and a display device (30). In one embodiment of the invention, the protected device (21) includes a microprocessor card placed in a box (22) (*e.g.*, a smart card placed into a smart card reader), and the display device (30) is a printer (*see, e.g.*, Specification, page 7, line 31 – page 8, line 31).

As discussed with reference to one embodiment of the present invention, when a message and its signature are sent to the recipient of the message, it is likely that the recipient will want to verify the certificate and the signature associated with the message (*see, e.g.*, Specification, page 11, lines 8-14). Accordingly, in one embodiment of the present invention, the protected device (21) checks the certificate and sends the display device (30) information, such as the validity of the certificate and the public key of the third party associated with the certificate (*see, e.g.*, Specification, page 11, line 36 – page 12, line 3).

Initially, rather than being directed toward using a hardware solution as claimed in the present invention, Kausik is actually directed toward a completely software solution using a method for camouflaging data by embedding it among many pieces of similar data (*see* Kausik,

col. 4, lines 11-15). Kausik clearly states that devices such as smart cards require expensive additional hardware infrastructure, have high administrative overhead for distribution and upkeep, and are inconvenient to the user (*see* Kausik, col. 3, lines 13-25). Therefore, a specific goal of Kausik is to overcome an assumed burden of having such additional hardware (*see* Kausik, col. 4, lines 45-65). Accordingly, the software-based key wallet of Kausik actually teaches away from the present invention.

The Examiner asserts that Kausik teaches a message, a signature, and a certificate are loaded ... onto a protected device connected to the storage device of the recipient (*see* Office Action dated July 12, 2005 at page 4). Applicant respectfully disagrees. Kausik merely discloses that a smart card contains a microprocessor and some memory, in which a user's private key and public key certificate are written. To use the card, the user enters a personal identification number (PIN) to activate the card (*see* Kausik, col. 2, lines 55-60).

The Examiner's attempt to equate the private key and public key certificate taught in Kausik to "a message, a signature, and a certificate" as recited in claims is completely nonsensical. In fact, a private key could not possibly be a message because a private key is used to sign or decrypt a message. Also, a private key could not possibly be a signature because a private key is actually used to calculate a signature. Further, a private key could not possibly be a certificate because a private key is most often associated with the public key which may be embedded in a certificate. Accordingly, no matter how broadly the claim language is read, "a message, a signature, and a certificate" as recited in claims cannot be equated to the private key and public key certificate taught in Kausik.

Further, Kausik is *completely silent* with respect to teaching "a protected device connected to the storage device of the recipient" as recited in the amended claim 1. As stated above, Kausik is directed to a software solution to the problem and does not contemplate loading

information onto a hardware device (*i.e.*, protected device). It appears that the Examiner is attempting to improperly read out the "protected device" limitation throughout this claim.

As discussed above, Kausik is *completely silent* with respect to a protected device. Accordingly, Kausik fails to teach checking a certificate within the protected device as recited in amended claim 1. Further, to the extent that Kausik discusses checking a certificate, Kausik merely discloses a known method or algorithm of certifying a public key, which allows a certificate holder to attach a public key certificate to an encrypted message. The identity of the sender and the authenticity of the public key are then verified by verifying the signature of the certifying authority (CA) associated with the public key certificate by using the CA's public key (*see* Kausik, col. 2, lines 25-37). This certification is not performed within the protected device.

Again, as discussed above, Kausik is *completely silent* with respect to a protected device. Therefore, Kausik clearly cannot teach calculation of a reduction of a message in a protected device.

Once again, as discussed above, Kausik is *completely silent* with respect to a protected device. Accordingly, Kausik necessarily cannot teach decrypting a signature in a protected device. Kausik merely states that a recipient of a message computes a hash of a received message in order to verify a signature attached to a message (*see* Kausik, col. 2, lines 15-19). It would be clear to one skilled in the art that the recipient of a message is not the same as a protected device, as discussed above.

Chaum, as discussed above with reference to Kausik, does not show or suggest all the limitations of amended independent claim 1. Further, Chaum does not show or suggest that which Kausik lacks. This is evidenced by the fact that Chaum is relied on only to teach "a method comprising verifying the identification of a card holder by sending information to a display device for verification" (See Office Action dated July 12, 2005 at page 4).

Further, as discussed above, because Kausik teaches that additional hardware is undesirable in the system of Kausik, one skilled in the art would have no motivation to combine Kausik with Chaum based on Chaum clearly discusses a small card-like hardware unit. Thus, without the present application as a guide, one skilled in the art would have no motivation to combine Kausik with Chaum.

In view of the above, Kausik and Chaum, (i) whether taken separately or in combination, fail to show or suggest the present invention as recited in amended independent claim 1, and (ii) are not properly combinable. Thus, amended independent claim 1 is patentable over Kausik and Chaum. Claims 2 and 3, depending directly from amended claim 1, are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Additionally, claims 4-6, dependent from amended independent claim 1, are allowable for at least the same reasons. Further, newly added claims 7-16, which contain language similar to claims 4-6, are allowable for at least the same reasons.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09669/009001).

Dated: October 12, 2005

Respectfully submitted,

By 

Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant